IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. No.:	09/668,421	Confirmation No. 2663
Applicant:	MOHAN ANANDA	
Filed:	September 22, 2000	
TC/A.U.:	3621	
Examiner:	CRISTINA O. SHERR	
Docket No.:	81045.913D3	
Customer No.:	22804	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Table of Contents

I. Real Parties In Interest

The real party in interest is Stamps.com, the assignee of the patent application.

II. Related Appeals and Interferences

None.

III. Status of Claims

Claims 1-197, 199-202, 205-212, 215, 217-218, 221 and 224-240 are cancelled. Claims 198, 203-204, 213-214, 216, 219-220, 222-223 and 241-243 are rejected. The rejections of claims 198, 203-204, 213-214, 216, 219-220, 222-223 and 241-243 are being appealed.

IV. Status of Amendments

No amendment has been filed subsequent to the final office action dated April 22, 2009 that is being appealed.

V. Summary of Claimed Subject Matter

There are two independent claims, 198 and 216.

Independent claim 198 is an apparatus claim. The subject matter of claim 198 is a system for transferring items having value (including software, postage, tickets, checks, coupons, certificates, etc.) over a computer network from a server system to a user terminal in response to a specific request from the user terminal for the item (Page 7, line 1 to Page 8, line 12; Page 14, line 20 to Page 15, line 17; Page 79, lines 9-16[1]). The server is configured to continuously verify the authentication of the request while the transfer takes place using the exchange of a non-

[1] The page and line numbers are from the patent application as originally filed.

predetermined pseudo random number parameter created specifically for the specific request. (Page 39, line 20 to Page 40, line 23). The terminal is configured to terminate the transfer if the authentication fails while the transfer is taking place (Page 15, lines 19-23).

Independent claim 216 is a method claim. The subject matter of claim 216 is a method for performing secure functions for an item having value in a computer network in response to a specific request for the function from a user terminal (Page 7, line 1 to Page 8, line 12; Page 14, line 20 to Page 15, line 17). The method includes the steps of continuing to verify authentication over time during performance of the secure functions using the exchange of a non-predetermined pseudo random number parameter created specifically for the specific request (Page 39, line 20 to Page 40, line 23), and terminating the performance of the secure functions if the authentication fails while the functions are being performed (Page 15, lines 19-23). Examples of the functions are generating and printing postage, tickets, checks, coupons, certificates, etc. (Page 79, lines 9-16).

The claims contain no means plus function or step plus function elements.

VI. Grounds of Rejection to be Reviewed on Appeal

Each of the grounds for rejection set forth by the Examiner in the final office action dated April 22, 2009 ("FOA") is to be reviewed on appeal. These grounds for rejection are as follows:

A. 35 U.S.C. 103 – Rejection of Claims 198, 213, 214, 216, 219, 220 and 241-243 as being Unpatentable over Whitehouse (U.S. Pat. No. 6,005,945) in View of Cordery et al. (U.S. Pat. No. 5,454,038)

The Examiner has rejected claims 198, 213, 214, 216, 219, 220 and 241-243 under 35 U.S.C. 103 as being unpatentable over Whitehouse (U.S. Pat. No. 6,005,945) in view of Cordery et al. (U.S. Pat. No. 5,454,038).

B. 35 U.S.C. 103 – Rejection of Claims 203-204 and 222-223 as being Unpatentable over Whitehouse (U.S. Pat. No. 6,005,945) in View of Cordery et al. (U.S. Pat. No. 5,454,038) and further in view of Kara (U.S. Pat. No. 5,822,739).

The Examiner has rejected claims 203-204 and 222-223 as being unpatentable over Whitehouse (U.S. Pat. No. 6,005,945) in view of Cordery et al. (U.S. Pat. No. 5,454,038) and further in view of Kara (U.S. Pat. No. 5,822,739).

VII. <u>Argument</u>

A. The Examiner Fails to Identify all of the Elements of Independent Claim 198 in the Prior Art in Rejecting Independent Claim 198 as being Unpatentable over Whitehouse (U.S. Pat. No. 6,005,945) in View of Cordery et al. (U.S. Pat. No. 5,454,038)

1. The Elements of Independent Claim 198

Independent claim 198 states[2]:

> 198. A system for transferring items having value in a computer network comprising:
>
> [(a)] a plurality of user terminals coupled to a computer network;
>
> [(b)] a database system coupled to said network and remote from said plurality of user terminals for storing information about one or more users using said plurality of user terminals; and
>
> [(c)] a server system coupled to said network, said server system comprising cryptographic capabilities for transferring an item having value to a user terminal issuing a specific request for said item having value utilizing said information stored in said database system, [(d)] wherein said server system is configured to continue verifying authentication of said specific request over time while said item having value is transferred to said user terminal and wherein [(e)] said user terminal is configured to terminate said transfer of said item having

[2] Identifying characters (e.g. "(a)", "(b)", etc.) have been added to aid in identifying specific claim elements. Those identifying characters are not included in the actual claims.

value if said authentication fails while said transfer is taking place, [(f)] said authentication comprising the exchange of a non-predetermined pseudo random number parameter created specifically for said specific request.

2. The Examiner Concedes that Whitehouse, the Examiner's Primary Reference, does not Disclose Elements (d), (e) and (f) of Independent Claim 198.

The Examiner concedes that elements (d), (e) and (f) of claim 198 are not disclosed by Whitehouse, but asserts that they are disclosed by Cordery. The Examiner states:

> 12. Whitehouse, does not specifically disclose, but Cordery does, [(d)] wherein said server system is configured to continue verifying authentication of said specific request over time while said item having value is transferred to said user terminal and wherein [(e)] said user terminal is configured to terminate said transfer of said item having value if said authentication fails while said transfer is taking place, [(f)] said authentication comprising the exchange of a non-predetermined pseudo random number parameter created specifically for said specific request. (e g col 9 ln 33- col 10 ln 39). Note that, as above, Cordery recites that "address hygiene may involve multiple communications between the mailer and the address hygiene data base" (col 9 ln 19-22). As above, "address hygiene may involve multiple communications between the mailer and the address hygiene data base" (col 9 ln 19-22). Note also that the mailer may "defer the processing of particular mailpieces requiring multiple communications" (col 9 in 33-38), thus terminating the transaction with respect to those mailpieces. Also, "uncorrected addresses can be outsorted from a mail run" (col 9 ln 40), thus terminating the transaction with respect to those mailpieces.
>
> 13. It would have been obvious, therefore, to a practitioner of ordinary skill in the art at the time the invention was made to add the authentication step of Cordery as well as the encryption/decryption method to that of Whitehouse for further enhancing the security of the communication in addition to better prevention of unauthorized requests as well as securing the storage of the data within the database using secret keys.
>
> (FOA, pp. 4-5, ¶¶12-13).

3. The Portions of Cordery Cited by the Examiner do not Disclose Elements (d), (e) and (f) of Independent Claim 198 as Asserted by the Examiner.

Elements (d), (e) and (f) recite a novel configuration of the claimed invention relating to authentication. Specifically, element (d) recites that the server system is configured to continue verification of authentication over time while the item of value in question is transferred to the user terminal. Element (e) recites that the user terminal is configured to terminate the transfer of the item having value if the authentication fails while the transfer is taking place. Element (f) recites that the authentication comprises the exchange of a non-predetermined pseudo random number parameter created specifically for the specific request for the item of value being transferred.

The portions of Cordery the Examiner cites as disclosing elements (d), (e) and (f) of claim 198 state as follows:

> col 9 ln 19-22
>
> Address hygiene may involve multiple communications between the mailer and the address hygiene data base.
>
> col 9 ln 30[3]- col 10 ln 46[4]
>
> This allows the mailer to generate all of the Digital Tokens for a large number of mailpieces which may be processed in a single time in one communication pass without the necessity to delay processing of the entire group of mailpieces until multiple communications with the address hygiened data base is completed or alternatively to defer the processing of the particular mailpieces requiring multiple communications.
>
> Alternatively, uncorrected address can be outsorted from a mail run so that all uncorrected addressed mail can be later processed, possibly as a separate batch with or without address correction.
>
> For those rating systems that provide a discount for hygiened addresses, it may be necessary for those unhygiened addresses (where uncorrected addresses or incomplete addresses are utilized) to pay an additional postage amount. Thus, the system must provide postage value to be imprinted by hygiened and unhygiened address as appropriate. An example, of an unhygiened address in the United States is where certain "vanity" names are used as opposed to standard names stored in the postal address data base.
>
> In areas where uncorrected addresses are utilized, it may be desirable to utilize an address identifier. This is a delivery address identifier to provide a unique

[3] Col 9, ln 33 of Cordery is in the middle of a sentence that begins on ln 30. For completeness, the entire sentence is reproduced.

[4] Col 10, ln 39 of Cordery is in the middle of a sentence that ends on ln 46. For completeness, the entire sentence is reproduced.

addressee number associated with a particular mailpiece (this may also be utilized in connection with hygiened addresses) which can be a numeric or alphanumeric string associated with the address. The string is derived algorithmically from the data in the delivery address block. It should be such that it is difficult to produce two different address blocks that have the same delivery address identifier. A Delivery Point Postal Code (such as a zip code in the United States which may involve up to 11 digits) is an example of a delivery address identifier.

At 604 a determination is made if there is another mailpiece for which a postage request is required. If this is true (as it would be for the first postage request received) the mailer at 606 generates the address for the mailpiece (which may be hygiened or unhygiened) and the various rating parameters as well as the date of entry into the mailstream (the date in which the mail will be deposited with the carrier). Other dates of entry can be used depending upon the nature of the system involved such as the date of creation of the mailpiece. The rating parameters can vary depending upon the particular rating system associated with the carrier involved. The rating systems vary from carrier to carrier, as for example the United States Postal Service, United Parcel Service, Federal Express, United Kingdom Royal Mail, etc. These services have various rating parameters utilized to determine the appropriate price for a delivery of a particular mailpiece (which for the purpose of the present invention and disclosure is intended to include parcels). At 606 the processing of a particular mailpiece is activated by generating various information elements that may include the address, rating parameters, date of entry. This may be appended to a postal request file which is being generated as various mailpieces loop through decision block 604 and are processed at 606. Where no further mailpieces are to be processed as determined at 604, communications is established with a remote data center at 608.

A procedure is initiated and completed at 610 to authenticate the data center in a known manner such that the mailer is assured that communication has been established with an authorized data center to issue the digital tokens to be printed on the mailpieces. Once this has been established, the postal request file may be encrypted at 612 and the encrypted postal data file transmitted at 614 to the data center. The data center at 616 performs its process on the transmitted encrypted postal request file as shown in detail in FIG. 7. This process at the data center which is shown in abbreviated form at block 616 and involves: generating (if a hygiened request has been made) a bad address file; a corrected address file; a postal revenue block file (with a postal revenue block associated with each of the plurality of mailpieces involved in the transmitted encrypted postal request file); and, an accounting record of the transaction which debits funds associated with the mailer's account for the digital tokens to be transmitted to the mailer. At 616 the data center encrypts (some or all) of the above noted files, namely, the bad address file, corrected address file, postage revenue block file and accounting record, and sends these files or portions thereof to the mailer.

a. The Portions of Cordery Cited by the Examiner do not Disclose a Server System Configured to Continue Verification of Authentication over Time While the Item of Value in Question is Transferred to the User Terminal as Recited in Element (d) of Claim 198.

The portions of Cordery cited by the Examiner do not disclose a server system that continues to verify authentication over time while an item having value is transferred to a user terminal as recited in element (d) of claim 198. Instead, Cordery discloses a "address hygiene process" in which a "data center" checks a list of addresses received from a "mailer" to make sure that each address is valid. If an address is invalid, the data center generates a corrected address if possible, or asks for more information to be able to determine the correct address.

The "address hygiene" process of Cordery does not involve continuous authentication over time, and specifically does not involve continuous authentication over time while an item of value is being transferred. The Examiner does not identify what the Examiner considers the "item of value" to be in the "address hygiene" process of Cordery. In the process of Cordery, as described in the above sections cited by the Examiner, the data center receives a list of addresses from the mailer. The data center checks the list of addresses against a valid address database. Any invalid addresses are added to a "bad address file," and are also corrected, if possible, and added to a "corrected address file." The data center also generates a file of "postage revenue blocks" ("Digital Tokens") for each address, and then sends the bad address, corrected address, and postage revenue block files to the mailer. (Cordery, col. 10, ln 34-47). Presumably, these files are what the Examiner contends are the "items having value" recited in claim 198. As disclosed by Cordery, the files may be encrypted <u>before</u> being sent to the mailer, but no authentication by the data server takes place <u>while the files are being transferred</u>, as required by element (d) of claim 198. Cordery describes nothing more than conventional encryption of a file before being sent and decryption of the file by the recipient after it is received. Cordery does not describe any authentication that takes place <u>while the file is being transferred</u>, as required by element (d) of claim 198. Accordingly, element (d) of claim 198 is not disclosed by Cordery.

b. The Portions of Cordery Cited by the Examiner do not Disclose a User Terminal Configured to Terminate the Transfer of an Item of Value if Authentication Fails While the Transfer is Taking Place as Recited in Element (e) of Claim 198.

The portions of Cordery cited by the Examiner do not disclose a user terminal that is configured to terminate the transfer of an item having value if continuous authentication fails while the transfer is taking place. As described above, the portions of Cordery cited by the Examiner disclose an "address hygiene process" in which the "data center" receives a list of addresses from the "mailer." The data center checks the list of addresses against a valid address database. Any invalid addresses are added to a "bad address file," and are also corrected, if possible, and added to a "corrected address file." The data center also generates a file containing "postal revenue blocks" for each address, and then sends all these files to the "mailer." (Cordery, col. 10, ln 34-47). As disclosed by Cordery, the files may be encrypted before being sent to the mailer, and decrypted by the mailer after being received, but no continuous authentication by the data server or the mailer takes place while the files are being transferred, as required by element (e) of claim 198.

The Examiner asserts that the statement in Cordery that the mailer may "defer the processing of particular mailpieces requiring multiple communications" is equivalent to "terminating the transactions with respect to those mailpieces" (FOA, p. 4, lines 20-22). Cordery is simply describing a situation in which the mailer, for efficiency purposes, processes the mailpieces that have correct addresses first, defering the processing of mailpieces that have incorrect addresses until later, because the correction of those addresses may involve multiple communications with the data center. Such a deferral is not a "termination" by the user terminal of a transfer of an item having value while the transfer is taking place due to the failure of continuous authentication as recited in element (e) of claim 198. Instead, it is simply a choice to defer processing of difficult mailpieces until after the processing of easy to process mailpieces has been completed.

Cordery does not describe a recipient user terminal[5] that is configured to terminate the transfer of an item having value if the continuous authentication fails while the item is being transferred, as required by element (e) of claim 198. Accordingly, element (e) of claim 198 is not disclosed by Cordery.

c. The Portions of Cordery Cited by the Examiner do not Disclose Continuous Authentication that Comprises the Exchange of a Non-Predetermined Pseudo Random Number Parameter Created Specifically for the Specific Request for the Item of Value being Transferred as Recited in Element (f) of Claim 198.

The portions of Cordery cited by the Examiner do not disclose continuous authentication, while a requested item of value is being transferred, that comprises the exchange of a non-predetermined pseudo random number parameter created specifically for the specific request for the item of value being transferred, as required by element (f) of claim 198. As described above, the portions of Cordery cited by the Examiner disclose nothing more than conventional encryption of a file before being sent and decryption of the file by the recipient after it is received. Cordery does not describe any continuous authentication that takes place while the file is being transferred, and specifically does not describe any continuous authentication that comprises the exchange of a non-predetermined pseudo random number created specifically for the specific request for the item of value being transferred, as required by element (f) of claim 198. Accordingly, element (f) of claim 198 is not disclosed by Cordery.

d. Because Cordery does not Disclose Any of the Claim Elements of Claim 198 that the Examiner Concedes are Missing from Whitehouse, the Combination of Whitehouse with Cordery does not Render Claim 198 Unpatentable over Whitehouse in View of Cordery.

As the Examiner concedes, Whitehouse does not disclose elements (d), (e) and (f) of independent claim 198. As shown above, Cordery does not disclose these missing elements either. Claim 198 is patentable if any one of its claim elements is missing from the prior art.

[5] The Examiner apparently considers the "mailer" of Cordery to correspond to the "user terminal" of claim 198.

Here, there are three elements missing in the combination of prior art cited by the Examiner. Accordingly, because the prior art combination cited by the Examiner lacks at least three distinct elements of independent claim 198 (namely elements (d), (e) and (f)), Whitehouse in view of Cordery does not, and cannot, render Claim 198 unpatentable. Claim 198 is therefore patentably distinct from Whitehouse in view of Cordery. The Examiner's rejection of Claim 198 under 35 U.S.C. §103 is in error.

B. The Examiner's Rejections of Dependent Claims 203-204 and 213-214 are Improper for the Same Reasons as the Rejection of Independent Claim 198

Dependent claims 203-204 and 213-214 are dependent on independent claim 198, and include all of the limitations of independent claim 198, as well as additional limitations. Accordingly, the Examiner's rejections of dependent claims 203-204 and 213-214 are improper for the same reasons as set forth above for independent claim 198.

C. The Examiner Fails to Identify all of the Elements of Independent Claim 216 in the Prior Art in Rejecting Independent Claim 216 as being Unpatentable over Whitehouse (U.S. Pat. No. 6,005,945) in View of Cordery et al. (U.S. Pat. No. 5,454,038)

1. The Elements of Independent Claim 216

Independent claim 216 states[6]:

> 216. A method for secure processing of items having value in a computer network comprising a plurality of user terminals comprising:
>
> [(a)] storing information about one or more users using a plurality of user terminals in a database system coupled to a network and remote from said plurality of user terminals; and

[6] Identifying characters (e.g. "(a)", "(b)", etc.) have been added to aid in identifying specific claim elements. Those identifying characters are not included in the actual claims.

[(b)] performing secure functions for an item having value in response to a specific request from a user terminal utilizing said information stored in said database system to execute cryptographic capabilities remote from said user terminal;

[(c)] continuing to verify authentication over time during performance of said secure functions for said item having value;

[(d)] terminating said performance of secure functions for said item having value if said authentication fails while said secure functions are being performed, [(e)] said authentication comprising the exchange of a non-predetermined pseudo random number parameter created specifically for said specific request.

2. The Examiner Concedes that Whitehouse, the Examiner's Primary Reference, does not Disclose Elements (c), (d) and (e) of Independent Claim 216

The Examiner concedes that elements (c), (d) and (e) of claim 216 are not disclosed by Whitehouse, but asserts that they are disclosed by Cordery. The Examiner states:

> 18. Whitehouse, does not specifically disclose, but Cordery does [(c)] continuing to verify authentication over time during performance of said secure functions for said item having value, and [(d)] terminating said performance of secure functions for said item having value if said authentication fails while said secure functions are being performed, [(e)] said authentication comprising the exchange of a non-predetermined pseudo random number parameter created specifically for said specific request. (e.g. col 9 ln 33- col 10 ln 39). Note that, as above, Cordery recites that "address hygiene may involve multiple communications between the mailer and the address hygiene data base" (col 9 ln 19-22). As above, "address hygiene may involve multiple communications between the mailer and the address hygiene data base" (col 9 ln 19-22). Note also that the mailer may "defer the processing of particular mailpieces requiring multiple communications" (col 9 ln 33-38), thus terminating the transaction with respect to those mailpieces. Also, "uncorrected addresses can be outsorted from a mail run . . ." (col 9 ln 40), thus terminating the transaction with respect to those mailpieces.
>
> 19. It would have been obvious, therefore, to a practitioner of ordinary skill in the art at the time the invention was made to add the authentication step of

> Cordery as well as the encryption/decryption method to that of Whitehouse for further enhancing the security of the communication in addition to better prevention of unauthorized requests as well as securing the storage of the data within the database using secret keys.
>
> (FOA, p. 6, ¶¶18-19)

3. The Portions of Cordery Cited by the Examiner do not Disclose Elements (c), (d) and (e) of Independent Claim 216 as Asserted by the Examiner.

The Examiner's argument regarding independent claim 216 is nearly identical to the Examiner's argument regarding independent claim 198, and the Examiner cites the same sections of Cordery. Even though the Appellant has already discussed those sections of Cordery with respect to independent claim 198 above, for completeness, Appellant will discuss them again in the context of the Examiner's rejection of independent claim 216.

Elements (c), (d) and (e) of independent claim 216 recite a novel configuration of the claimed invention relating to authentication. Specifically, element (c) recites that verification of authentication is continued over time <u>during the requested performance of the secure functions</u> (such as, for example, transferring the item to a user terminal) for the item having value. Element (d) recites that performance of the secure function (e.g. transferring the item having value) is terminated if authentication fails <u>while the secure function is being performed</u>. Element (e) recites that the authentication comprises the exchange of a <u>non-predetermined</u> pseudo random number parameter <u>created specifically for the specific request</u> for the secure function being performed.

The portions of Cordery the Examiner cites as disclosing elements (c), (d) and (e) of claim 216 state as follows:

> <u>col 9 ln 19-22</u>
>
> Address hygiene may involve multiple communications between the mailer and the address hygiene data base.

col 9 ln 30[7]- col 10 ln 46[8]

This allows the mailer to generate all of the Digital Tokens for a large number of mailpieces which may be processed in a single time in one communication pass without the necessity to delay processing of the entire group of mailpieces until multiple communications with the address hygiened data base is completed or alternatively to defer the processing of the particular mailpieces requiring multiple communications.

Alternatively, uncorrected address can be outsorted from a mail run so that all uncorrected addressed mail can be later processed, possibly as a separate batch with or without address correction.

For those rating systems that provide a discount for hygiened addresses, it may be necessary for those unhygiened addresses (where uncorrected addresses or incomplete addresses are utilized) to pay an additional postage amount. Thus, the system must provide postage value to be imprinted by hygiened and unhygiened address as appropriate. An example, of an unhygiened address in the United States is where certain "vanity" names are used as opposed to standard names stored in the postal address data base.

In areas where uncorrected addresses are utilized, it may be desirable to utilize an address identifier. This is a delivery address identifier to provide a unique addressee number associated with a particular mailpiece (this may also be utilized in connection with hygiened addresses) which can be a numeric or alphanumeric string associated with the address. The string is derived algorithmically from the data in the delivery address block. It should be such that it is difficult to produce two different address blocks that have the same delivery address identifier. A Delivery Point Postal Code (such as a zip code in the United States which may involve up to 11 digits) is an example of a delivery address identifier.

At 604 a determination is made if there is another mailpiece for which a postage request is required. If this is true (as it would be for the first postage request received) the mailer at 606 generates the address for the mailpiece (which may be hygiened or unhygiened) and the various rating parameters as well as the date of entry into the mailstream (the date in which the mail will be deposited with the carrier). Other dates of entry can be used depending upon the nature of the system involved such as the date of creation of the mailpiece. The rating parameters can vary depending upon the particular rating system associated with the carrier involved. The rating systems vary from carrier to carrier, as for example the United States Postal Service, United Parcel Service, Federal Express, United

[7] Col 9, ln 33 of Cordery is in the middle of a sentence that begins on ln 30. For completeness, the entire sentence is reproduced.

[8] Col 10, ln 39 of Cordery is in the middle of a sentence that ends on ln 46. For completeness, the entire sentence is reproduced.

> Kingdom Royal Mail, etc. These services have various rating parameters utilized to determine the appropriate price for a delivery of a particular mailpiece (which for the purpose of the present invention and disclosure is intended to include parcels). At 606 the processing of a particular mailpiece is activated by generating various information elements that may include the address, rating parameters, date of entry. This may be appended to a postal request file which is being generated as various mailpieces loop through decision block 604 and are processed at 606. Where no further mailpieces are to be processed as determined at 604, communications is established with a remote data center at 608.
>
> A procedure is initiated and completed at 610 to authenticate the data center in a known manner such that the mailer is assured that communication has been established with an authorized data center to issue the digital tokens to be printed on the mailpieces. Once this has been established, the postal request file may be encrypted at 612 and the encrypted postal data file transmitted at 614 to the data center. The data center at 616 performs its process on the transmitted encrypted postal request file as shown in detail in FIG. 7. This process at the data center which is shown in abbreviated form at block 616 and involves: generating (if a hygiened request has been made) a bad address file; a corrected address file; a postal revenue block file (with a postal revenue block associated with each of the plurality of mailpieces involved in the transmitted encrypted postal request file); and, an accounting record of the transaction which debits funds associated with the mailer's account for the digital tokens to be transmitted to the mailer. At 616 the data center encrypts (some or all) of the above noted files, namely, the bad address file, corrected address file, postage revenue block file and accounting record, and sends these files or portions thereof to the mailer.

a. The Portions of Cordery Cited by the Examiner do not Disclose Verification of Authentication that is Continued Over Time During the Performance of a Secure Function for an Item Having Value as Recited in Element (c) of Claim 216.

The portions of Cordery cited by the Examiner do not disclose verification of authentication that is continued over time during the performance of a secure function for an item having value as recited in element (c) of claim 216. Instead, Cordery discloses a "address hygiene process" in which a "data center" checks a list of addresses received from a "mailer" to make sure that each address is valid. If an address is invalid, the data center generates a corrected address if possible, or asks for more information to be able to determine the correct address.

The "address hygiene" process of Cordery does not involve continuous authentication over time, and specifically does not involve continuous authentication over time while a secure function is performed for an item having value. The Examiner does not identify what the Examiner considers the "item of value" to be in the "address hygiene" process of Cordery. Also, the Examiner does not identify what function in Cordery is the "secure function" for the "item having value" recited in claim 216.

In the process of Cordery, as described in the above sections cited by the Examiner, the data center receives a list of addresses from the mailer. The data center checks the list of addresses against a valid address database. Any invalid addresses are added to a "bad address file," and are also corrected, if possible, and added to a "corrected address file." The data center also generates a file of "postage revenue blocks" ("Digital Tokens") for each address, and then sends the bad address, corrected address, and postage revenue block files to the mailer. (Cordery, col. 10, ln 34-47). Presumably, one or more of these files are what the Examiner contends is the "item having value" recited in claim 216, and, presumably, the transmission of these files to the "mailer" of Cordery is what the Examiner considers to be the "secure function."

As disclosed by Cordery, the files may be encrypted before being sent to the mailer, but no contiunous verification of authentication takes place while the secure function is being performed, as required by element (c) of claim 216. Cordery describes nothing more than conventional encryption of a file before being sent and decryption of the file by the recipient after it is received. Cordery does not describe any authentication that takes place while the secure function is being performed, as required by element (c) of claim 216. Accordingly, element (c) of claim 216 is not disclosed by Cordery.

b. The Portions of Cordery Cited by the Examiner do not Disclose terminating the Performance of Secure Functions for an Item Having Value if Authentication Fails While the Secure Functions are being Performed as Recited in Element (d) of Claim 216.

The portions of Cordery cited by the Examiner do not disclose terminating the performance of secure functions for an item having value if authentication fails while the secure functions are being performed. As described above, the portions of Cordery cited by the Examiner disclose an "address hygiene process" in which the "data center" receives a list of addresses from the "mailer." The data center checks the list of addresses against a valid address database. Any invalid addresses are added to a "bad address file," and are also corrected, if possible, and added to a "corrected address file." The data center also generates a file containing "postal revenue blocks" for each address, and then sends all these files to the "mailer." (Cordery, col. 10, ln 34-47). As disclosed by Cordery, the files may be encrypted <u>before</u> being sent to the mailer, and decrypted by the mailer <u>after</u> being received, but no <u>continuous</u> authentication by the data server or the mailer takes place <u>while secure functions are being performed</u>, as required by element (d) of claim 216.

The Examiner asserts that the statement in Cordery that the mailer may "defer the processing of particular mailpieces requiring multiple communications" is equivalent to "terminating the transactions with respect to those mailpieces" (FOA, p. 4, lines 20-22). Cordery is simply describing a situation in which the mailer, for efficiency purposes, processes the mailpieces that have correct addresses first, defering the processing of mailpieces that have incorrect addresses until later, because the correction of those addresses may involve multiple communications with the data center. Such a deferral is not a "termination" of secure functions for an item having value <u>while the functions are being performed</u> due to the failure of <u>continuous authentication</u> as recited in element (d) of claim 216. Instead, it is simply a choice to defer <u>processing</u> of difficult mailpieces until after the processing of easy to process mailpieces has been completed.

Cordery does not describe terminating performance of secure functions for an item having value if continuous verification of authentication fails while the secure functions are being performed, as required by element (d) of claim 216. Accordingly, element (d) of claim 216 is not disclosed by Cordery.

c. The Portions of Cordery Cited by the Examiner do not Disclose Continuous Authentication that Comprises the Exchange of a Non-Predetermined Pseudo Random Number Parameter Created Specifically for the Specific Request for Performance the Secure Functions for the Item of Value as Recited in Element (e) of Claim 216.

The portions of Cordery cited by the Examiner do not disclose continuous authentication, while a secure function for an item of value is being performed, that comprises the exchange of a non-predetermined pseudo random number parameter created specifically for the specific request for the performance of the secure functions for the item of value, as required by element (e) of claim 216. As described above, the portions of Cordery cited by the Examiner disclose nothing more than conventional encryption of a file before being sent and decryption of the file by the recipient after it is received. Cordery does not describe any continuous authentication that takes place while the file is being transferred (or while any other secure function is performed for an item having value), and specifically does not describe any continuous authentication that comprises the exchange of a non-predetermined pseudo random number created specifically for the specific request for the secure functions being performed on the item of value, as required by element (e) of claim 216. Accordingly, element (e) of claim 216 is not disclosed by Cordery.

d. Because Cordery does not Disclose Any of the Claim Elements of Claim 216 that the Examiner Concedes are Missing from Whitehouse, the Combination of Whitehouse with Cordery does not Render Claim 216 Unpatentable over Whitehouse in View of Cordery.

As the Examiner concedes, Whitehouse does not disclose elements (c), (d) and (e) of independent claim 216. As shown above, Cordery does not disclose these missing elements either. Claim 216 is patentable if any one of its claim elements is missing from the prior art.

Here, there are three elements missing in the combination of prior art cited by the Examiner. Accordingly, because the prior art combination cited by the Examiner lacks at least three distinct elements of independent claim 216 (namely elements (c), (d) and (e)), Whitehouse in view of Cordery does not, and cannot, render Claim 216 unpatentable. Claim 216 is therefore patentably distinct from Whitehouse in view of Cordery. The Examiner's rejection under 35 U.S.C. §103 is in error.

D. The Examiner's Rejections of Dependent Claims 219-220, 222-223 and 241-243 are Improper for the Same Reasons as the Rejection of Independent Claim 216

Dependent claims 219-220, 222-223 and 241-243 are dependent on independent claim 216, and include all of the limitations of independent claim 216, as well as additional limitations. Accordingly, the Examiner's rejections of dependent claims 219-220, 222-223 and 241-243 are improper for the same reasons as set forth above for independent claim 216.

E. Conclusion

For the reasons set forth above, appellant believes that the Examiner's rejections of claims 198, 203-204, 213-214, 216, 219-220, 222-223 and 241-243 are improper and should be overturned by the Board. Applicant believes that all pending claims 198, 203-204, 213-214, 216, 219-220, 222-223 and 241-243 are in condition for allowance, and respectfully requests that the Board order that they be allowed.

Respectfully Submitted,

THE HECKER LAW GROUP

Date: December 16, 2009

By: ______________

Frank M. Weyer
Reg. No. 33,050

VIII. CLAIMS APPENDIX

198. A system for transferring items having value in a computer network comprising:

a plurality of user terminals coupled to a computer network;

a database system coupled to said network and remote from said plurality of user terminals for storing information about one or more users using said plurality of user terminals; and

a server system coupled to said network, said server system comprising cryptographic capabilities for transferring an item having value to a user terminal issuing a specific request for said item having value utilizing said information stored in said database system, wherein said server system is configured to continue verifying authentication of said specific request over time while said item having value is transferred to said user terminal and wherein said user terminal is configured to terminate said transfer of said item having value if said authentication fails while said transfer is taking place, said authentication comprising the exchange of a non-predetermined pseudo random number parameter created specifically for said specific request.

203. The system of claim 198, wherein said server system comprising said cryptographic capabilities further comprises a cryptographic device that generates a digital signature in response to said specific user request.

204. The system of claim 198, wherein said server system comprising said cryptographic capabilities further comprises a cryptographic device that encrypts said item having value.

213. The system of claim 198, wherein said cryptographic capabilities comprise a cryptographic device that protects data using a stored secret.

214. The system of claim 213, wherein said secret is a password.

216. A method for secure processing of items having value in a computer network comprising a plurality of user terminals comprising:

storing information about one or more users using a plurality of user terminals in a database system coupled to a network and remote from said plurality of user terminals; and

performing secure functions for an item having value in response to a specific request from a user terminal utilizing said information stored in said database system to execute cryptographic capabilities remote from said user terminal;

continuing to verify authentication over time during performance of said secure functions for said item having value;

terminating said performance of secure functions for said item having value if said authentication fails while said secure functions are being performed, said authentication comprising the exchange of a non-predetermined pseudo random number parameter created specifically for said specific request.

219. The method of claim 216 further comprising authenticating the identity of a user.

220. The method of claim 219 further comprising verifying that the authenticated user is authorized to print said item having value.

222. The method of claim 216, wherein said cryptographic capabilities are provided by a cryptographic device configured to generate a digital signature in response to said specific request.

223. The method of claim 216, wherein said cryptographic capabilities are provided by a cryptographic device configured to encrypt said item having value.

241. The system of claim 198, wherein said server system comprising said cryptographic capabilities further comprises a cryptographic device that encrypts said item having value in response to said specific request.

242. The method of claim 220 further comprising verifying that said authenticated user is authorized to request transfer said item having value.

243. The method of claim 216, wherein said cryptographic capabilities are configured to encrypt the requested information in response to said specific request for transferring said item having value.

IX. EVIDENCE APPENDIX

None.

X. RELATED PROCEEDINGS APPENDIX

None.